AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1-32 (Cancelled)

33. (Currently Amended) An apparatus comprising:

an interface to at least one wired client device to receive Secure Sockets Layer (SSL) encrypted data and at least one wireless client device to receive Wireless Transport Layer Security (WTLS) encrypted data;

client-type determining logic to determine whether a client device requesting a secure connection is a wired client device or a wireless client device;

logic to perform a wired authentication to establish the secure connection when it is determined that the requesting client device is a wired client device;

logic to perform a wireless authentication to establish the secure connection when it is determined that the requesting client device is a wireless client device; and

logic to convert the SSL encrypted data to an unencrypted format and to convert the WTLS encrypted data an unencrypted format, wherein the conversions are based on a conversion indication received [[from]] through the interface.

34. (Currently Amended) The apparatus of claim 33, implemented within a data center, and further comprising an interface to transmit data in the unencrypted format to, and to receive data in an unencrypted format from, a server within the data center.

35. (Previously Presented) The apparatus of claim 33, wherein the logic to perform the wired authentication comprises logic to perform authentication using a wired communication protocol,

and wherein the logic to perform the wireless authentication comprises logic to perform authentication using a wireless communication protocol.

36. (Previously Presented) The apparatus of claim 35, wherein the logic to perform the wired authentication comprises logic to perform authentication using a Public Key Infrastructure (PKI) protocol and wherein the logic to perform the wireless authentication comprises logic to perform authentication using a Wireless Public Key Infrastructure (WPKI) protocol.

37. (Previously Presented) The apparatus of claim 33, wherein the logic to perform the wired authentication and the logic to perform the wireless authentication each comprises:

logic to determine if a requesting client device has requested authentication of the server; and

logic to transmit a server digital certificate for the server when it is determined that the requesting client device has requested authentication of the server.

38. (Previously Presented) The apparatus of claim 33, wherein the logic to perform the wired authentication and the logic to perform the wireless authentication each comprises:

logic to generate a request for a digital certificate from a requesting client device; and

logic to authenticate a digital certificate received from a client device.

39. (Previously Presented) The apparatus of claim 33, wherein the logic to perform the wired authentication and the logic to perform the wireless authentication each comprises:

logic to retrieve a client digital certificate using a Uniform Resource Locator received from the client device; and

logic to authenticate a retrieved client digital certificate.

40. (Previously Presented) The apparatus of claim 33, wherein the client-type determining logic comprises:

logic to determine a security protocol used for an encrypted request from a client device; and

logic to determine whether the requesting client device is a wired client device or a wireless client device dependent on the determined security protocol.

41. (Previously Presented) The apparatus of claim 33, further comprising:

logic to receive a client digital signature from the client device; and

logic to validate the received client digital signature.

42. (Previously Presented) A method comprising:

receiving data within a data center from at least one wired client device and at least one wireless client device each requesting a secure connection with a server of the data center;

performing a wired authentication to establish the secure connection with the wired client device; and

performing a wireless authentication to establish the secure connection with the wireless client device; and

converting the data from an encrypted format to an unencrypted format based on a received conversion indication.

43. (Previously Presented) The method of claim 42, wherein said performing the wired authentication comprises performing authentication using a wired communication protocol and wherein the performing the wireless authentication comprises performing authentication using a wireless communication protocol.

44. (Previously Presented) The method of claim 42, wherein said performing the wired authentication and said performing the wireless authentication each comprises:

determining if a requesting client device has requested authentication of the server; and

transmitting a server digital certificate for the server when it is determined that the requesting client device has requested authentication of the server.

45. (Previously Presented) The method of claim 42, wherein each of said performing the wired authentication and said performing the wireless authentication comprises:

generating a request for a digital certificate from a requesting client device; and

authenticating a digital certificate received from a client device.

46. (Previously Presented) The method of claim 45, wherein said authenticating a digital certificate includes verifying a validity period of the client digital certificate.

47. (Previously Presented) The method of claim 42, wherein each of said performing the wired authentication and said performing the wireless authentication comprises:

retrieving a client digital certificate using a Uniform Resource Locator received from the client device; and

authenticating a retrieved client digital certificate.

48. (Previously Presented) The method of claim 42, further comprising:

determining a security protocol used for an encrypted request from a client device; and

determining whether the requesting client device is a wired client device or a wireless client device dependent on the determined security protocol.

49. (Previously Presented) The method of claim 42, further comprising:

receiving a client digital signature from a client device; and

validating the received client digital signature.

50. (Currently Amended) An article comprising a machine-readable medium having stored thereon instructions that if executed cause a machine to perform operations comprising:

receiving first encrypted data from at least one wired client device and second encrypted data from at least one wireless client device each requesting a secure connection with a server;

performing a wired authentication to establish the secure connection with the wired client device; and

performing a wireless authentication to establish the secure connection with the wireless client device; and

converting ~~logic to convert~~ the first encrypted data to a plain data format and converting ~~to convert~~ the second encrypted data to a plain data format based on a conversion indication received at the machine ~~from at the server~~.

51. (Previously Presented) The article of claim 50, wherein the instructions to perform the wired authentication further comprise instructions that if executed cause the machine to perform operations comprising authentication using Public Key Infrastructure (PKI) protocol, and wherein the instructions to perform the wireless authentication further comprise instructions that if executed cause the machine to perform operations comprising authenticating using Wireless Public Key Infrastructure (WPKI) protocol.

52. (Previously Presented) The article of claim 50, wherein the instructions to perform each of the wired authentication and the wireless authentication comprise instructions that if executed cause the machine to perform operations comprising:

generating a request for a digital certificate from a requesting client device; and

authenticating a digital certificate received from a client device.

53. (Previously Presented) The method of claim 42, further comprising updating a short-lived server certificate from a certificate authority repository based on a user defined interval.

54. (Previously Presented) The method of claim 42, wherein said performing the wired authentication comprises performing the wired authentication based on Public Key Infrastructure (PKI), and wherein said performing the wireless authentication comprises performing the wireless authentication based on Wireless Public Key Infrastructure (WPKI).

55. (Previously Presented) The method of claim 42, further comprising:

performing a security format conversion for encrypted data received from the wired device; and

performing a security format conversion for encrypted data received from the wireless device.

56. (Currently Amended) An apparatus comprising:

a network interface to receive Secure Sockets Layer (SSL) data from a wired device through a public network and Wireless Transport Layer Security (WTLS) data from a wireless device through a public network;

Public Key Infrastructure (PKI) logic to establish a secure connection with the wired device;

Wireless Public Key Infrastructure (WPKI) logic to establish a secure connection with the wireless device;

SSL logic to convert the SSL data to another format;

WTLS logic to convert the WTLS data to another format, wherein the conversions are based on a received conversion indication; and

a second interface to provide the data converted from the SSL and WTLS formats to a data center server over a private network.

57. (Currently Amended) The apparatus of claim 56, wherein the apparatus is to reside in [[a]] the data center between [[a]] the public network and [[a]] the data center server.

58. (Previously Presented) The apparatus of claim 56, wherein the other format is a plain data format, and wherein the PKI logic, the WPKI logic, the SSL logic, and the WTLS logic are all included within a single device.